TRANSFORMATION NUMERIQUE

Session 5 : se mettre en conformité RGPD

Mardi 27 juin
14h00-16h00

27/06/2023

SOMMAIRE

VOTRE INTERVENANT

Guillaume Jasson du Fantastique Bazar

Guillaume Jasson

Co-fondateur du Fantastique Bazar, expert du numérique associatifs, il accompagne les associations dans leur transformation digitale depuis plus de 5 ans

Organisation

Le Fantastique Bazar est une ESS experte du numérique associatif. Elle accompagne depuis plus de 4 ans des associations de toute taille pour construire une stratégie digitale, concevoir des plateformes digitales et développer sites et applications métiers.

OBJECTIFS PÉDAGOGIQUES

De la session d'aujourd'hui
Durée de la formation : 2H

OBJECTIF 1

Comprendre ce qu'est le RGPD

OBJECTIF 2

Comprendre comment marche la mise en conformité

OBJECTIF 3

Pouvoir lancer une démarche de mise en conformité RGPD

CALENDRIER DE LA FORMATION

12
MAI

SESSION 1

Quelle place pour le numérique dans mon projet à impact

14
FÉVRIER

SESSION 2

Le no-code pour les projets à impact

14
MARS

SESSION 3

Gagner du temps en automatisant son activité

24
MAI

SESSION 4

Bien rédiger un cahier des charges numérique

27
JUIN

SESSION 5

Se mettre en conformité RGPD

Thomas Barwick/Getty Images

1

Définition et délimitation du sujet

Qui s'y connaît déjà en RGPD ?

Le RGPD – Règlement Général de Protection des Données

C’est quoi ?

C’est un règlement qui s’applique dans toute l’Union Européenne (UE) et à tous les citoyens de l’UE et toutes les personnes morales qui exercent une activité au sein de l’UE. Il porte sur la manière dont les entreprises et autres organisations doivent se comporter vis-à-vis des données personnelles.

Ca concerne qui ?

Toute structure qui rassemble des données personnelles non anonymisées.

Ca concerne quoi ?

Toutes les données personnelles que vous possédez, digitales ou non.

Comment ça fonctionne ?

Ce règlement se base sur la responsabilité individuelle et l'auto-contrôle.

2 grandes responsabilités : **identifier** et **protéger** les données personnelles que l'on possède.

LA CIRCULATION DES DONNÉES

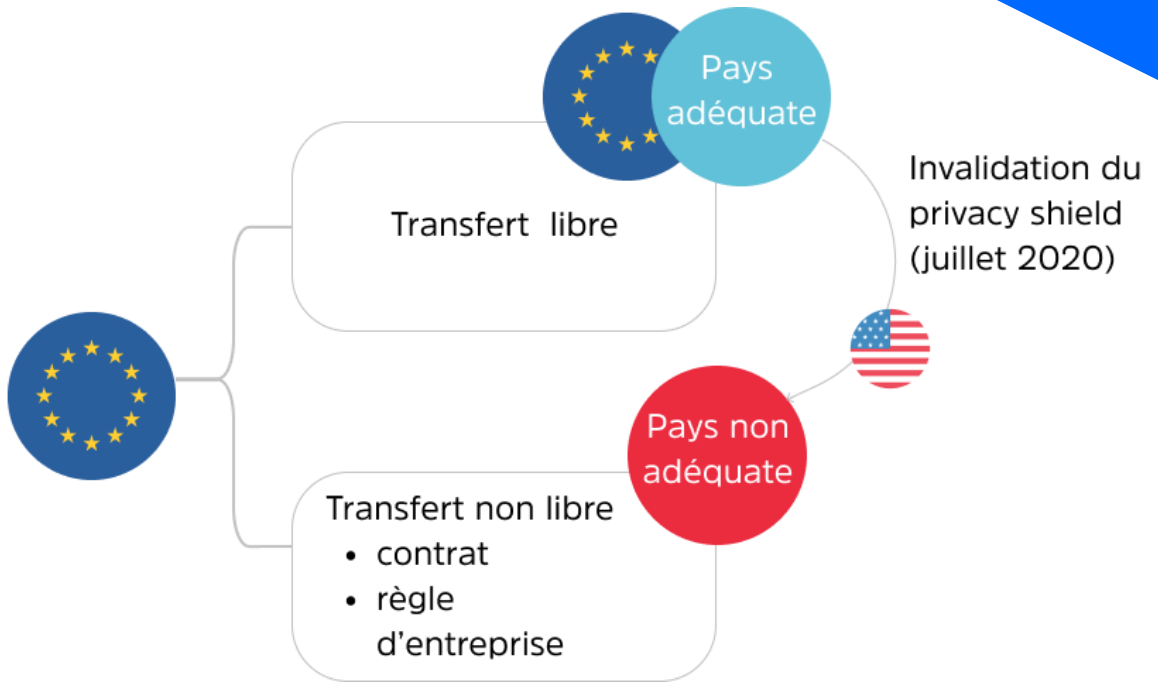
Toutes ces règles portent sur les données personnelles circulant librement au sein de l'UE

Le RGPD prend le dessus sur les juridictions des États membres de l'Union Européenne.

Ce règlement place le standard européen au dessus de ses voisins contre lesquels le RGPD protège les citoyens européens en imposant des règles de circulation en fonction de chaque pays.

Hors UE, il y a 2 types de pays :

- les pays adéquates
- les pays non adéquates



Des questions sur l'équivalence de protection ?

DONNÉES PERSONNELLES ET LISTE DE DONNÉES

Une donnée personnelle, kesako ?

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable

3 PARAMÈTRES

1. Une liste

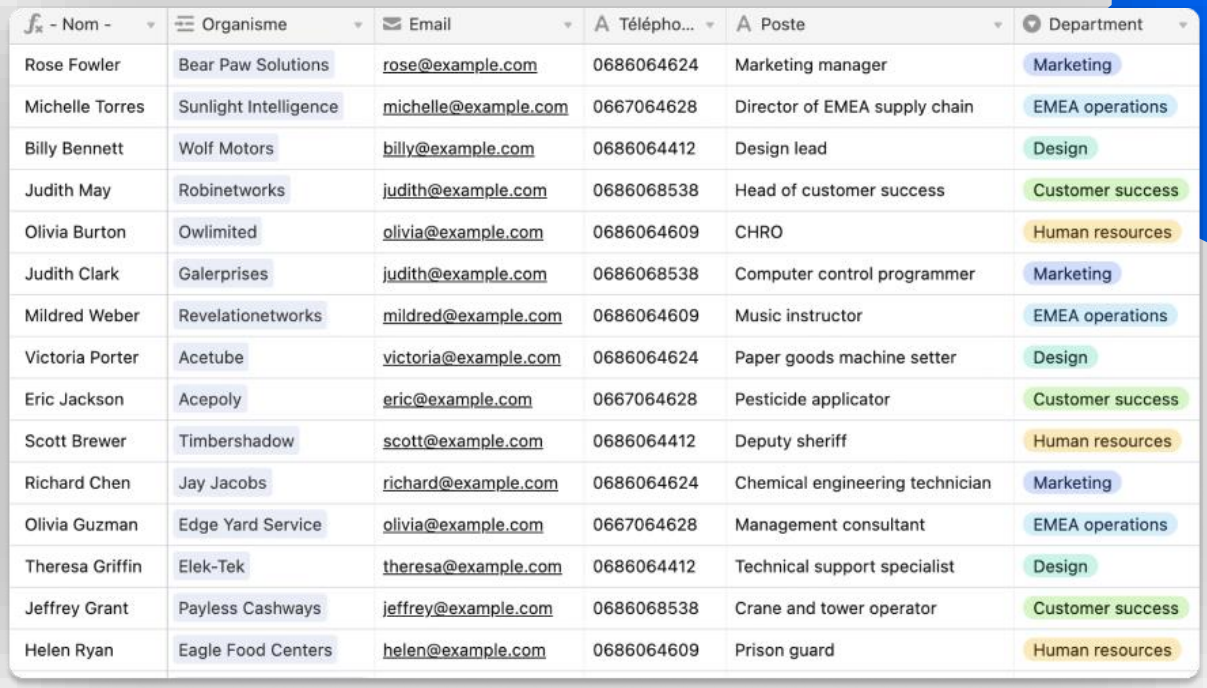
La répétition du même format de contenu à l'identique

2. Des données

Cette liste contient des informations (pas des objets)

3. Personnelles

Les données se rapportent à des personnes (pas des objets par exemple)



- Nom -	Organisme	Email	Télépho...	Poste	Department
Rose Fowler	Bear Paw Solutions	rose@example.com	0686064624	Marketing manager	Marketing
Michelle Torres	Sunlight Intelligence	michelle@example.com	0667064628	Director of EMEA supply chain	EMEA operations
Billy Bennett	Wolf Motors	billy@example.com	0686064412	Design lead	Design
Judith May	Robinetworks	judith@example.com	0686068538	Head of customer success	Customer success
Olivia Burton	Owlimited	olivia@example.com	0686064609	CHRO	Human resources
Judith Clark	Galerprises	judith@example.com	0686068538	Computer control programmer	Marketing
Mildred Weber	Revelationetworks	mildred@example.com	0686064609	Music instructor	EMEA operations
Victoria Porter	Acetube	victoria@example.com	0686064624	Paper goods machine setter	Design
Eric Jackson	Acepoly	eric@example.com	0667064628	Pesticide applicator	Customer success
Scott Brewer	Timbershadow	scott@example.com	0686064412	Deputy sheriff	Human resources
Richard Chen	Jay Jacobs	richard@example.com	0686064624	Chemical engineering technician	Marketing
Olivia Guzman	Edge Yard Service	olivia@example.com	0667064628	Management consultant	EMEA operations
Theresa Griffin	Elek-Tek	theresa@example.com	0686064412	Technical support specialist	Design
Jeffrey Grant	Payless Cashways	jeffrey@example.com	0686068538	Crane and tower operator	Customer success
Helen Ryan	Eagle Food Centers	helen@example.com	0686064609	Prison guard	Human resources

Quelles liste de données personnelles vous identifiez dans votre asso ?

Exemples – Newsletter et autres

Un outil de newsletter est un outil de communication qui permet de construire des mails types et de les envoyer périodiquement à une liste de destinataires qui ont consenti à recevoir ces mails

Cela nécessite a minima de collecter des mails mais souvent on y ajoute des noms, des informations spécifiques pour personnaliser le contenu.

Dans cet outil, la base contact est une liste de données personnelles

Autres exemples:

- Liste du personnel
- Liste des bénéficiaires
- Liste des bénévoles
- Liste des donateurs
- Liste des financeurs
- etc.

DONNÉES PERSONNELLES ≠ DONNÉES SENSIBLES

Les données sensibles, c'est une catégorie particulière des données personnelles, soumises à un régime spécifique

On y retrouve les informations d'une personne physique sur :

- Les données de santé ;
- Les données sur des personnes mineures ;
- La prétendue origine raciale ou ethnique, les opinions politiques ;
- Les convictions religieuses ou philosophiques ou l'appartenance syndicale ;
- Les données génétiques, les données biométriques ;
- La vie sexuelle ou l'orientation sexuelle.

Leur récolte et conservation est soit interdite soit soumise à un régime plus contraignant (consentement spécifique, manifestation rendue publique, protocole de sécurité renforcé, utilisation justifiée et validée par la CNIL)

Caractéristiques d'un cahier des charges

1

Ça permet de définir ses besoins

C'est dans le cahier des charges que l'on définit qui l'on est, ou l'on veut aller, et pour quoi on a besoin d'une plateforme web

2

Ça permet de sélectionner ses prestataires

Un cahier des charges bien rédigé vous permet de recevoir des réponses qualifiées qui vous permettent de choisir le prestataire le mieux qualifié pour répondre à vos besoins

3

Ça cadre la mission

C'est également un document de référence tout au long de la mission sur des sujets de conflit

2

Collecte et conservation de données

LES BASES LÉGALES

Les bases légales, ce sont les raisons qui vous donnent le droit de conserver des données.

1

Consentement

La personne vous autorise librement et en connaissance de cause à collecter et conserver ses données personnelles

2

Intérêt légitime

Pour protéger les intérêts légitimes de collecteur de données (garantir la sécurité informatique, la lutte contre la fraude, etc.)

LES BASES LÉGALES

3

Nécessaire à l'exécution du contrat

Dans l'hypothèse où l'absence de données personnelles vous empêche de remplir vos obligations vis-à-vis de la personne qui ne vous les donne pas

4

Mission d'intérêt public

Concerne surtout le traitement effectué par les personnes publiques. Mais va s'étendre aux sous traitants du service public (concession, délégation de service public)

5

Sauvegarde des intérêts vitaux

Principalement dans le cadre d'un contexte médical

LE CONSENTEMENT

Le consentement est la base légale principale que l'on va utiliser

Le recueil du consentement des personnes autorise le traitement de leurs données par les responsables du traitement.

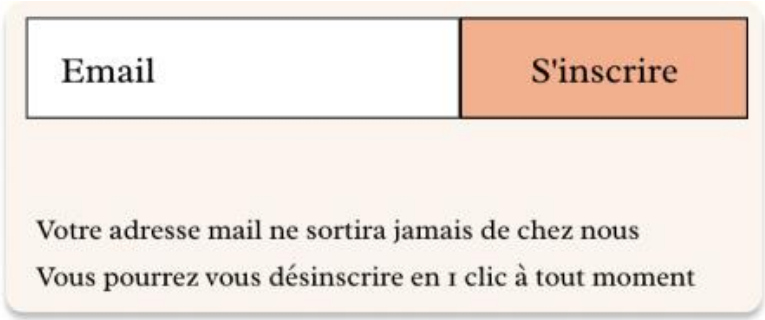
Il doit être mis en avant et être recueilli dans des conditions particulières assurant sa validité

Il doit explicitement permettre aux personnes :

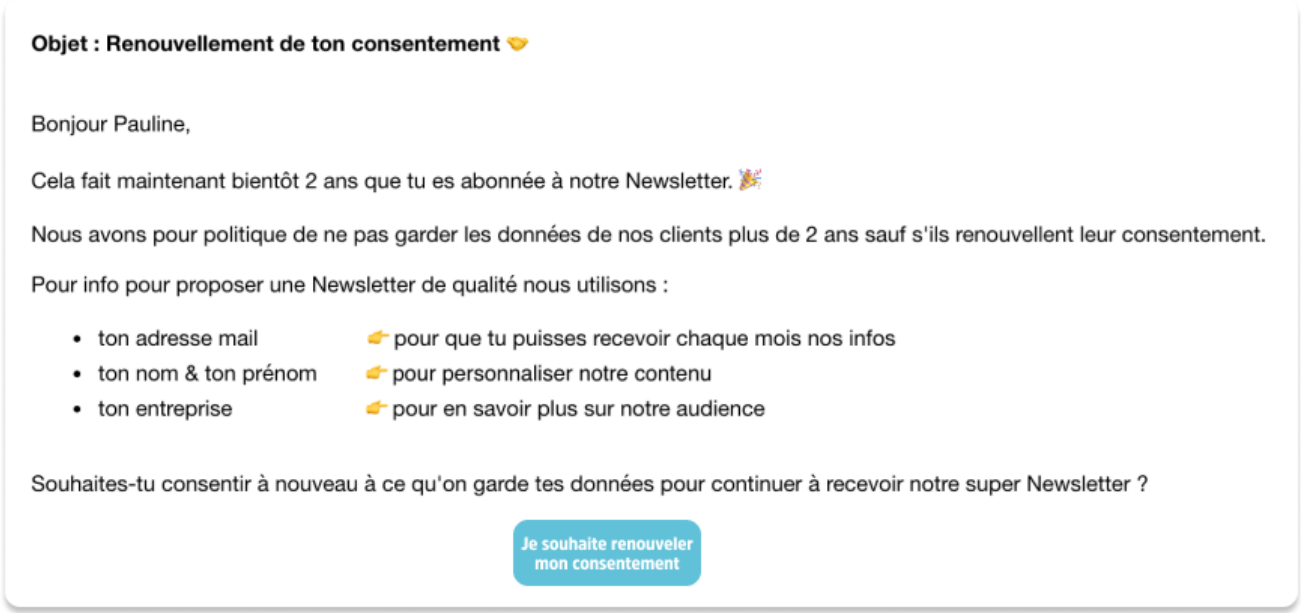
- De comprendre le traitement qui sera fait de leurs données (quelles données, pour quoi, pour combien de temps) ;
- De choisir sans contrainte d'accepter ou non ce traitement ;
- De changer d'avis librement.

EN PRATIQUE ÇA DONNE QUOI ?

Expliquer simplement les modalités de traitement



S'assurer régulièrement du consentement



L'INTÉRÊT LÉGITIME

Le champs est plus restrictif que ça ne laisse entendre

L'intérêt légitime est une des bases légales sur laquelle peut se fonder un traitement de données personnelles sans demande de consentement au préalable

Le recours à l'intérêt légitime est soumis à 3 conditions :

- L'intérêt poursuivi par l'organisme doit être « légitime » (gestion admin interne, sécurité du réseau, prévention de la fraude,…)
- L'intérêt légitime ne peut être retenu que si le traitement satisfait à la condition de « nécessité »
- Le traitement ne doit pas heurter les droits et intérêts des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables

A ce stade, qui s'y retrouve encore et qui a des questions ?

3

La pratique au quotidien

QUI S'EN OCCUPE ?

Le/la responsable de traitement

La personne, l'autorité publique, la société ou l'organisme qui détermine les finalités et les moyens de ce fichier, qui décide de sa création. Il s'agit généralement de la personne morale incarnée par son représentant légal.

Dans le cadre associatif : c'est l'association elle-même et donc in fine son représentant légal

Le/la délégué.e à la protection des données

Le responsable de traitement peut être appuyé par un DPD (anciennement CIL et DPO en anglais).

Il aide à l'esprit RGPD dans la structure et facilite les échanges avec la CNIL, il n'est cependant pas juridiquement responsable en cas de non conformité.

Il est obligatoire pour les organismes publics et certaines entreprises aux activités bien spécifiques à grande échelle (suivi de personnes, traitement de données sensibles)

LE REGISTRE DES DONNÉES

Chaque structure qui traite des données doit tenir à jour un registre de données.

Il recense, analyse et reflète la réalité du traitement des données personnelles.

Il est composé d'une fiche par activité.

Une fiche contient les informations suivantes :

- Les parties prenantes ;
- Les catégories de données traitées ;
- L'utilisation des données ;
- Le temps de conservation ;
- La sécurisation.

EXEMPLE

Description du traitement	
Nom du traitement	Gestion de la paie
N° / RÉF	1 - Exemple
Date de création du traitement	26/05/2018
Mise à jour du traitement	13/05/2019

Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	Louise DUPONT	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	exemple1@ets.com
Délégué à la protection des données	Martin HENRI	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	exemple2@ets.com
Société du DPO (si celui-ci est externe)	N/A						

Finalité(s) du traitement effectué	
Finalité principale	Gestion de la paie
Sous-finalité 1	Calcul des rémunérations
Sous-finalité 2	Calcul du montant des versements adressés aux organismes sociaux
Sous-finalité 3	Ordre de virement à la banque

Catégories de données personnelles concernées	Description	Durée de conservation
État civil, identité, données d'identification, images...	Noms, prénoms, adresses	5 ans à compter du versement de la paie
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter du versement de la paie
Numéro de Sécurité Sociale (ou NIR)	Numéros de sécurité sociale des salariés	5 ans à compter du versement de la paie

Catégories de personnes concernées	Description	Précisions
Catégorie de personnes 1	Salariés	

Destinataires	Type de destinataire	Précisions
Destinataire 1	Service interne qui traite les données	Dir. Administrative et Financière
Destinataire 2	Partenaires institutionnels ou commerciaux	Organismes sociaux
Destinataire 3	Destinataires dans des pays tiers ou organisations internationale	Banque d'Andorre

Mesures de sécurité	Type de mesure de sécurité	Précisions
Mesure de sécurité 1	Mesures de protection des logiciels	
Mesure de sécurité 2	Sauvegarde des données	
Mesure de sécurité 3	Contrôle d'accès des utilisateurs	

Transferts hors UE	Destinataire	Pays	Type de Garanties	Liens vers la documentation
Organisme destinataire 1	Banque d'Andorre	Andorre	Clauses contractuelles types (CCT)	Contrat en date du 23/01/2018

LA SOUS-TRAITANCE

Le sous-traitant est la personne physique ou morale qui traite des données pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation (Ex : organisme de gestion des paies)

Mention obligatoires dans les contrats des sous-traitants

- Transparence et traçabilité
- Protection des données dès la conception et par défaut
- Garantie de la sécurité des données traitées
- Assistance, alerte et conseil

ET POUR L'UTILISATEUR

Les personnes dont vous conservez les données ont des droits

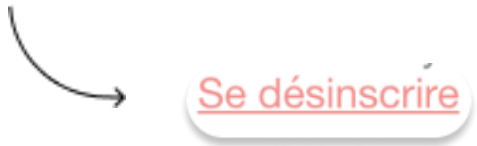
Le RGPD protège les personnes dont les données sont collectées et leur prodigue des droits afin qu'elles restent en contrôle de leurs données personnelles.

Elles peuvent donc exercer sur votre organisme

- Le droit d'opposition
- Les droits d'accès et de rectification
- Le droit à la portabilité

Pour vous ça veut dire qu'a minima il faut :

- Communiquer une adresse mail pour recevoir les réclamations
- Permettre de se désinscrire facilement



4

Lancer sa mise en conformité

Chronologie classique d'un projet web

Etape 1

Nommer un DPD (ou DPO)

Il exercera une mission d'information, de conseil et de contrôle en interne

Etape 2

FAIRE UN INVENTAIRE DES DONNÉES

- Identifier toutes les listes de données
- Identifier leur contenu et leur destination

Etape 3

DÉFINIR LA POLITIQUE DE RÉCOLTE ET DE TRAITEMENT

- Définir quelles données, pour quoi faire, pour combien de temps pour chaque liste.
- Pour chaque donnée identifier les bases légales.

Etape 4

CRÉER ET REMPLIR LE REGISTRE

A partir du modèle de la CNIL ou d'un autre modèle, reporter les listes de données et leurs caractéristiques

Chronologie classique d'un projet web

Etape 5

FAIRE UNE CAMPAGNE DE CONSENTEMENT

Les données que vous souhaitez conserver sur la base légale du consentement doivent faire l'objet d'un consentement exprès et éclairé

Etape 6

PROGRAMMER LES DATE DS DE RENOUVELLEMENT DU CONSENTEMENT

Anticiper la date de renouvellement

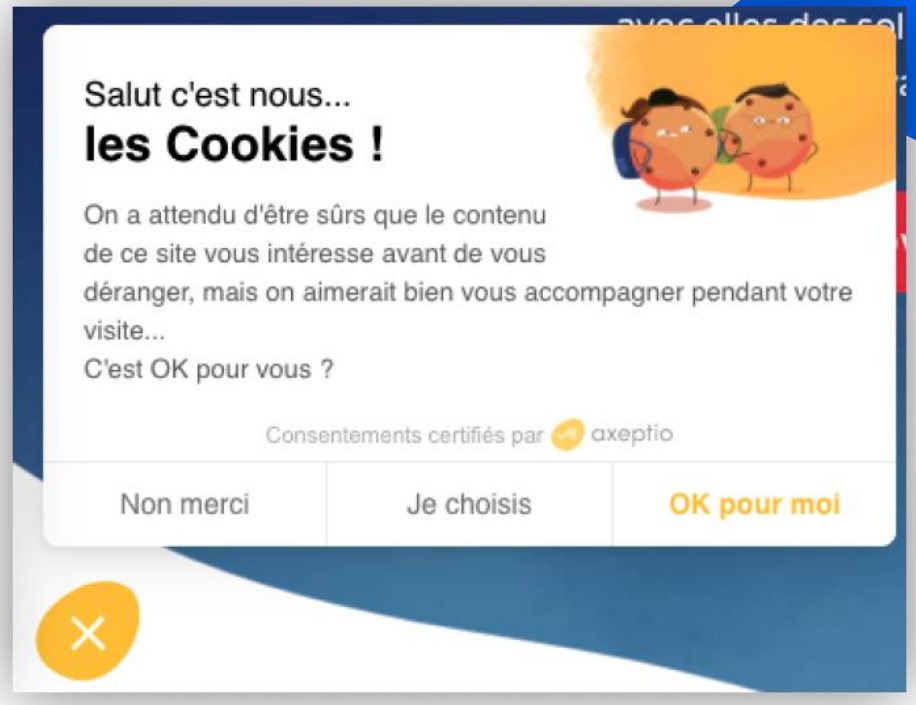
Et les cookies dans tout ça ?

Définition

C’est un fichier stocké par le site internet qui comporte des informations sur vous et vos données de navigation. Très souvent, il y a des données personnelles

Notre recommandation : Axeptio

- Il est vraiment facile et sympa à utiliser par les visiteurs du site (discret, clair, chaleureux, tout ce qu’on aime)
- Il est abordable
- Il est simple à installer
- Il est français



QUIZZ TIME !

AIDEZ-NOUS

A améliorer les prochaines sessions

SVP, prenez 5 minutes après la session pour l'évaluer.

Lien vers le questionnaire ici : https://form.jotform.com/231723471350348

RESSOURCES ET RÉFÉRENCES

Pour aller plus loin

- Centre de ressource de la Plateforme d'accompagnement Impact 2024
- N'hésitez pas à contacter l'agence Tada ! fondée par Amélie Cembalo qui accompagne des associations sur la mise en conformité RGPD. Elle propose également des formations et une newsletter spécifiquement sur la mise en conformité RGPD.

- Le Fantastique Bazar :
  - La Newsletter par ici
  - Le podcast par là
  - Les formations numérique gratuites toutes les deux semaines ici

UN GRAND MERCI

A VOUS !

CONTACT

Guillaume JASSON
Fantastique Bazar
guillaume@fantastiquebazar.com